I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS EXPRESS MAIL #EL098882599US IN AN ENVELOPE ADDRESSED TO: ASSISTANT COMMISSIONER FOR PATENTS, BOX PATENT APPLICATION, WASHINGTON, D.C. 20231, ON THE DATE INDICATED BELOW.

BY: Frances Sebuabey DATE: 02/13/01

#2

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of: **YOSHIAKI KAWATSURA et al.**

Serial No. N/A

Group Art Unit: N/A

Filed: Herewith

Examiner: N/A

Entitled: APPARATUS AND METHOD FOR DISTRIBUTION OF CONTENTS

Attorney Docket #: 080017.0008

jc821 U.S. PTO 09/782319 02/13/01

CLAIM OF FOREIGN PRIORITY AND TRANSMITTAL OF PRIORITY DOCUMENT

Applicant(s) hereby claim(s) the right of foreign priority under 35 U.S.C. Section 119 for the above-identified patent application. The claim of foreign priority is based upon Application No. 2000-218408, filed in Japan on July 19, 2000, and the benefit of that date is claimed.

Submitted herewith is a certified copy of Japan Application No. 2000-218408. It is submitted that this document completes the requirements of 35 U.S.C. Section 119, and benefit of the foreign priority is respectfully requested.

Respectfully submitted,

Yoshiaki KAWATSURA

February 13, 2001
(Date)

By: Alex Chartove

ALEX CHARTOVE, ESQ./ Registration No. 31,942;
Customer No. 000027000
AKIN, GUMP, STRAUSS, HAUER & FELD, L.L.P.
1333 New Hampshire Avenue, N.W.; Suite 400
Washington, D.C. 20036
Telephone: (202) 887-0000
Direct Dial: (202) 887-4149
Facsimile: (202) 955-7613
E-Mail: achartove@akingump.com

Attorney for Applicant

AC/fs
Enclosures

Patent Office
Japanese Government

This is to certify that the annexed is a true copy of the following application as filed with this office.

Date of Application : July 19, 2000
Application Number: P2000-218408

Application (s): Hitachi, Ltd.

Dated this 6th day of October 2000

Kozo Oikawa
Patent Office

Certificate No. 2000-3081690

340000410 US1

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年 ７月１９日

出願番号
Application Number: 特願２０００－２１８４０８

出願人
Applicant (s): 株式会社日立製作所

２０００年１０月 ６日

特許庁長官
Commissioner,
Patent Office 及川耕造

【書類名】　特許願

【整理番号】　H0000410

【あて先】　特許庁長官殿

【国際特許分類】　G06F 19/00

【発明者】

【住所又は居所】　神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所　ビジネスソリューション開発本部内

【氏名】　川連　嘉晃

【発明者】

【住所又は居所】　神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所　ビジネスソリューション開発本部内

【氏名】　千葉　寛之

【発明者】

【住所又は居所】　神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所　ビジネスソリューション開発本部内

【氏名】　渡邉　清

【発明者】

【住所又は居所】　神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所　ビジネスソリューション開発本部内

【氏名】　森田　光

【発明者】

【住所又は居所】　神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所　ビジネスソリューション開発本部内

【氏名】　富山　朋哉

【発明者】

【住所又は居所】　神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所　ビジネスソリューション開発本部内

【氏名】　坪　毅

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社日立製作所

【代理人】

【識別番号】　100096954

【弁理士】

【氏名又は名称】　矢島　保夫

【手数料の表示】

【予納台帳番号】　022781

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　コンテンツ提供方法及び装置

【特許請求の範囲】

【請求項１】

受取者装置と資格授与者装置とコンテンツ提供者装置とを接続した通信ネットワークを用いたコンテンツ提供方法であって、

前記受取者装置において、取得したいコンテンツに関する要求情報を前記資格授与者装置に送付するステップと、

前記資格授与者装置において、前記コンテンツに関する要求情報に関連したチケットデータを受取者の公開鍵を用いて暗号化し、その暗号化チケットデータに対し資格授与者の秘密鍵を用いて電子署名を行なった後、前記暗号化チケットデータとその電子署名情報を前記受取者装置に送付するステップと、

前記受取者装置において、前記暗号化チケットデータを受取者の秘密鍵を用いて復号し、復号したチケットデータと前記暗号化チケットデータと前記電子署名情報とを前記コンテンツ提供者装置に送付するステップと、

前記コンテンツ提供者装置において、資格授与者の公開鍵を用いて前記電子署名情報を検証し、前記チケットデータを受取者の公開鍵で暗号化し、前記暗号化チケットデータとの整合性を確認した後、受取者装置へ送るべきコンテンツ情報を受取者の公開鍵で暗号化し、その暗号化コンテンツ情報を前記受取者装置へ送付するステップと、

前記受取者装置において、前記暗号化コンテンツ情報を受取者の秘密鍵で復号するステップと

を備えたことを特徴とするコンテンツ提供方法。

【請求項２】

受取者装置と資格授与者装置とコンテンツ提供者装置とを接続した通信ネットワークを用いたコンテンツ提供方法であって、

前記受取者装置において、受取者の公開鍵および取得したいコンテンツに関する要求情報を前記資格授与者装置に送付するステップと、

前記資格授与者装置において、前記コンテンツに関する要求情報に関連したチ

ケットデータを前記受取者の公開鍵を用いて暗号化し、その暗号化チケットデータに対し資格授与者の秘密鍵を用いて電子署名を行なった後、前記暗号化チケットデータとその電子署名情報を前記受取者装置に送付するステップと、

前記受取者装置において、前記暗号化チケットデータを受取者の秘密鍵を用いて復号し、復号したチケットデータと前記暗号化チケットデータと前記電子署名情報と前記受取者の公開鍵とを前記コンテンツ提供者装置に送付するステップと、

前記コンテンツ提供者装置において、資格授与者の公開鍵を用いて前記電子署名情報を検証し、前記チケットデータを前記受取者の公開鍵で暗号化し、前記暗号化チケットデータとの整合性を確認した後、受取者装置へ送るべきコンテンツ情報を前記受取者の公開鍵で暗号化し、その暗号化コンテンツ情報を前記受取者装置へ送付するステップと、

前記受取者装置において、暗号化コンテンツ情報を受取者の秘密鍵で復号するステップと

を備えたことを特徴とするコンテンツ提供方法。

【請求項３】

請求項１または２に記載のコンテンツ提供方法において、

前記コンテンツ提供者装置による前記暗号化チケットデータの整合性の確認後、受取者に関する情報取得の為の入力フォームを前記コンテンツ提供者装置から前記受取者装置に送るステップと、

前記受取者装置において、前記入力フォームに対応する情報を受取者が入力することにより入力済みフォームを生成し、受取者の秘密鍵を用いて電子署名を施して前記コンテンツ提供者装置に送るステップと、

前記コンテンツ提供者装置において、前記電子署名を受取者装置の公開鍵を用いて検証した後、前記コンテンツ情報を受取者の公開鍵で暗号化した暗号化コンテンツ情報を前記受取者装置へ送付するステップと

をさらに備えたことを特徴とするコンテンツ提供方法。

【請求項４】

請求項１から３の何れか１つに記載のコンテンツ提供方法において、

前記資格授与者装置が前記受取者装置に前記暗号化チケットデータを送る際、資格授与者の公開鍵を含み資格授与者を客観的に証明する証明書を添付し、

前記受取者装置が前記コンテンツ提供者装置に前記チケットデータを送る際、前記資格授与者の証明書を添付し、

前記コンテンツ提供者装置は、前記資格授与者の証明書を検証するとともに、前記資格授与者の電子署名情報を検証する際、前記資格授与者の証明書から取得した資格授与者の公開鍵を用いる

ことを特徴とするコンテンツ提供方法。

【請求項５】

受取者装置と資格授与者装置とコンテンツ提供者装置とを通信ネットワークを介して接続したコンテンツ提供システムであって、

前記受取者装置は、取得したいコンテンツに関する要求情報を前記資格授与者装置に送付する手段と、前記資格授与者装置から送られてくる暗号化チケットデータを受取者の秘密鍵を用いて復号する手段と、復号したチケットデータと前記暗号化チケットデータとその電子署名情報とを前記コンテンツ提供者装置に送付する手段と、前記コンテンツ提供者装置から送られてくる暗号化コンテンツ情報を受取者の秘密鍵で復号する手段とを備え、

前記資格授与者装置は、前記コンテンツに関する要求情報に関連したチケットデータを受取者の公開鍵を用いて暗号化する手段と、その暗号化チケットデータに対し資格授与者の秘密鍵を用いて生成した電子署名情報を付す手段と、前記暗号化チケットデータとその電子署名情報を前記受取者装置に送付する手段とを備え、

前記コンテンツ提供者装置は、資格授与者の公開鍵を用いて前記電子署名情報を検証する手段と、前記チケットデータを受取者の公開鍵で暗号化し、前記暗号化チケットデータとの整合性を確認する手段と、受取者装置へ送るべきコンテンツ情報を受取者の公開鍵で暗号化し、その暗号化コンテンツ情報を前記受取者装置へ送付する手段とを備えたことを特徴とするコンテンツ提供システム。

【請求項６】

受取者装置と資格授与者装置とコンテンツ提供者装置とを通信ネットワークを

介して接続したコンテンツ提供システムであって、

前記受取者装置は、受取者の公開鍵および取得したいコンテンツに関する要求情報を前記資格授与者装置に送付する手段と、前記資格授与者装置から送られてくる暗号化チケットデータを受取者の秘密鍵を用いて復号する手段と、復号したチケットデータと前記暗号化チケットデータとその電子署名情報と前記受取者の公開鍵とを前記コンテンツ提供者装置に送付する手段と、前記コンテンツ提供者装置から送られてくる暗号化コンテンツ情報を受取者の秘密鍵で復号する手段とを備え、

前記資格授与者装置は、前記コンテンツに関する要求情報に関連したチケットデータを受取者の公開鍵を用いて暗号化する手段と、その暗号化チケットデータに対し資格授与者の秘密鍵を用いて生成した電子署名情報を付す手段と、前記暗号化チケットデータとその電子署名情報を前記受取者装置に送付する手段とを備え、

前記コンテンツ提供者装置は、資格授与者の公開鍵を用いて前記電子署名情報を検証する手段と、前記チケットデータを受取者の公開鍵で暗号化し、前記暗号化チケットデータとの整合性を確認する手段と、受取者装置へ送るべきコンテンツ情報を受取者の公開鍵で暗号化し、その暗号化コンテンツ情報を前記受取者装置へ送付する手段とを備えたことを特徴とするコンテンツ提供システム。

【請求項７】

請求項５または６に記載のコンテンツ提供システムにおいて、

前記コンテンツ提供者装置による前記暗号化チケットデータの整合性の確認後、受取者に関する情報取得の為の入力フォームを前記コンテンツ提供者装置から前記受取者装置に送る手段と、

前記受取者装置において、前記入力フォームに対応する情報を受取者が入力することにより入力済みフォームを生成し、受取者の秘密鍵を用いて電子署名を施して前記コンテンツ提供者装置に送る手段と、

前記コンテンツ提供者装置において、前記電子署名を受取者装置の公開鍵を用いて検証した後、前記コンテンツ情報を受取者の公開鍵で暗号化した暗号化コンテンツ情報を前記受取者装置へ送付する手段と

をさらに備えたことを特徴とするコンテンツ提供システム。

【請求項８】

請求項５から７の何れか１つに記載のコンテンツ提供システムにおいて、

前記資格授与者装置における前記受取者装置に前記暗号化チケットデータを送付する手段は、送付するデータに、資格授与者の公開鍵を含み資格授与者を客観的に証明する証明書を含め、

前記受取者装置における前記コンテンツ提供者装置に前記チケットデータを送付する手段は、送付するデータに、前記資格授与者の証明書を含め、

前記コンテンツ提供者装置における前記電子署名情報を検証する手段は、前記資格授与者の証明書を検証するとともに、前記資格授与者の電子署名情報を検証する際、前記資格授与者の証明書から取得した資格授与者の公開鍵を用いるものである

ことを特徴とするコンテンツ提供システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コンテンツ提供方法及び装置に関し、特に通信ネットワークを利用した、コンテンツの取得資格の有無を検証するコンテンツ提供方法及び装置に関する。

【０００２】

【従来の技術】

コンテンツ受取者と提供者の二者間において、通信ネットワークを用いて各種のコンテンツを授受する際には、正しい受取者であることを検証したい場合がある。このような場合は、コンテンツの受取者がコンテンツ提供者に対して当該コンテンツの要求を行い、コンテンツ提供者は当該コンテンツを受け取るのに妥当な受取者かどうかを検証した後に、受取者がコンテンツを受け取るのが、一般的である。また、ネットワーク上でのパスワードの盗み見や、受け取りコンテンツの横取りを防止する為には、通信路を暗号化するための手段であるSSL(Secure Socket Layer)を用いるのが一般的である。

【０００３】

また、現在国際的な標準化団体であるIETF(Internet Engineer Task Force)で標準化が行われている取引プロトコルIOTP(Internet Open Trading Protocol)では、コンテンツの受取資格授与者と当該コンテンツの提供者が分離しており、受取資格授与者に相当するサーバからコンテンツの情報や取得資格情報を取得し、その情報をコンテンツ提供者へ送ってコンテンツを取得する。

【０００４】

【発明が解決しようとする課題】

かかる従来の方法においては、次のような問題がある。

【０００５】

まず、二者間でのコンテンツ授受の場合においては、コンテンツ提供者が複数存在した場合、それらコンテンツを一括管理する窓口の役割を果たす第三者機関を設ける場合がある。この場合、その第三者機関が当該コンテンツを複製して使用する可能性がある。また、各コンテンツ提供者がコンテンツ提供時に受取者に関する情報（物品送付の場合の住所や、アンケート情報など）を取得したい場合には、窓口たる第三者機関を通し、間接的に受け取ることになる為、第三者に改ざんされても分からない。

【０００６】

また、IOTPにおいては、現状では本当に受取者が正当かどうかを検証する機構が存在しない。したがって、これまでのデータを受取者が他の人に渡した場合にその人がコンテンツを受け取れてしまう可能性がある。

【０００７】

本発明の目的は、コンテンツの受取資格授与者と提供者を明確に分離することにより受取資格授与者が授与対象コンテンツデータを管理することを避け、その上で受取資格授与者が権利を与えた当該受取者のみが安全に受け取ることができるコンテンツ提供方法及び装置を提供することにある。

【０００８】

また本発明の他の目的は、正当なコンテンツ受取者からの情報を正確にコンテンツ提供者が受け取ることが出来るコンテンツ提供方法及び装置を提供すること

にある。

【０００９】

【課題を解決するための手段】

上記目的を達成するため、本発明は、受取者装置と資格授与者装置とコンテンツ提供者装置とを接続した通信ネットワークを用いたコンテンツ提供方法であって、前記受取者装置において、取得したいコンテンツに関する要求情報を前記資格授与者装置に送付するステップと、前記資格授与者装置において、前記コンテンツに関する要求情報に関連したチケットデータを受取者の公開鍵を用いて暗号化し、その暗号化チケットデータに対し資格授与者の秘密鍵を用いて電子署名を行なった後、前記暗号化チケットデータとその電子署名情報を前記受取者装置に送付するステップと、前記受取者装置において、前記暗号化チケットデータを受取者の秘密鍵を用いて復号し、復号したチケットデータと前記暗号化チケットデータと前記電子署名情報とを前記コンテンツ提供者装置に送付するステップと、前記コンテンツ提供者装置において、資格授与者の公開鍵を用いて前記電子署名情報を検証し、前記チケットデータを受取者の公開鍵で暗号化し、前記暗号化チケットデータとの整合性を確認した後、受取者装置へ送るべきコンテンツ情報を受取者の公開鍵で暗号化し、その暗号化コンテンツ情報を前記受取者装置へ送付するステップと、前記受取者装置において、前記暗号化コンテンツ情報を受取者の秘密鍵で復号するステップとを備えたことを特徴とする。

【００１０】

また本発明は、受取者装置と資格授与者装置とコンテンツ提供者装置とを接続した通信ネットワークを用いたコンテンツ提供方法であって、前記受取者装置において、受取者の公開鍵および取得したいコンテンツに関する要求情報を前記資格授与者装置に送付するステップと、前記資格授与者装置において、前記コンテンツに関する要求情報に関連したチケットデータを前記受取者の公開鍵を用いて暗号化し、その暗号化チケットデータに対し資格授与者の秘密鍵を用いて電子署名を行なった後、前記暗号化チケットデータとその電子署名情報を前記受取者装置に送付するステップと、前記受取者装置において、前記暗号化チケットデータを受取者の秘密鍵を用いて復号し、復号したチケットデータと前記暗号化チケッ

トデータと前記電子署名情報と前記受取者の公開鍵とを前記コンテンツ提供者装置に送付するステップと、前記コンテンツ提供者装置において、資格授与者の公開鍵を用いて前記電子署名情報を検証し、前記チケットデータを前記受取者の公開鍵で暗号化し、前記暗号化チケットデータとの整合性を確認した後、受取者装置へ送るべきコンテンツ情報を前記受取者の公開鍵で暗号化し、その暗号化コンテンツ情報を前記受取者装置へ送付するステップと、前記受取者装置において、暗号化コンテンツ情報を受取者の秘密鍵で復号するステップとを備えたことを特徴とする。

【００１１】

また本発明は、上述のコンテンツ提供方法において、前記コンテンツ提供者装置による前記暗号化チケットデータの整合性の確認後、受取者に関する情報取得の為の入力フォームを前記コンテンツ提供者装置から前記受取者装置に送るステップと、前記受取者装置において、前記入力フォームに対応する情報を受取者が入力することにより入力済みフォームを生成し、受取者の秘密鍵を用いて電子署名を施して前記コンテンツ提供者装置に送るステップと、前記コンテンツ提供者装置において、前記電子署名を受取者装置の公開鍵を用いて検証した後、前記コンテンツ情報を受取者の公開鍵で暗号化した暗号化コンテンツ情報を前記受取者装置へ送付するステップとをさらに備えたことを特徴とする。

【００１２】

また本発明は、上述のコンテンツ提供方法において、前記資格授与者装置が前記受取者装置に前記暗号化チケットデータを送る際、資格授与者の公開鍵を含み資格授与者を客観的に証明する証明書を添付し、前記受取者装置が前記コンテンツ提供者装置に前記チケットデータを送る際、前記資格授与者の証明書を添付し、前記コンテンツ提供者装置は、前記資格授与者の証明書を検証するとともに、前記資格授与者の電子署名情報を検証する際、前記資格授与者の証明書から取得した資格授与者の公開鍵を用いることを特徴とする。

【００１３】

さらに本発明は、受取者装置と資格授与者装置とコンテンツ提供者装置とを通信ネットワークを介して接続したコンテンツ提供システムであって、前記受取者

装置は、取得したいコンテンツに関する要求情報を前記資格授与者装置に送付する手段と、前記資格授与者装置から送られてくる暗号化チケットデータを受取者の秘密鍵を用いて復号する手段と、復号したチケットデータと前記暗号化チケットデータとその電子署名情報とを前記コンテンツ提供者装置に送付する手段と、前記コンテンツ提供者装置から送られてくる暗号化コンテンツ情報を受取者の秘密鍵で復号する手段とを備え、前記資格授与者装置は、前記コンテンツに関する要求情報に関連したチケットデータを受取者の公開鍵を用いて暗号化する手段と、その暗号化チケットデータに対し資格授与者の秘密鍵を用いて生成した電子署名情報を付す手段と、前記暗号化チケットデータとその電子署名情報を前記受取者装置に送付する手段とを備え、前記コンテンツ提供者装置は、資格授与者の公開鍵を用いて前記電子署名情報を検証する手段と、前記チケットデータを受取者の公開鍵で暗号化し、前記暗号化チケットデータとの整合性を確認する手段と、受取者装置へ送るべきコンテンツ情報を受取者の公開鍵で暗号化し、その暗号化コンテンツ情報を前記受取者装置へ送付する手段とを備えたことを特徴とする。

【００１４】

さらに本発明は、受取者装置と資格授与者装置とコンテンツ提供者装置とを通信ネットワークを介して接続したコンテンツ提供システムであって、前記受取者装置は、受取者の公開鍵および取得したいコンテンツに関する要求情報を前記資格授与者装置に送付する手段と、前記資格授与者装置から送られてくる暗号化チケットデータを受取者の秘密鍵を用いて復号する手段と、復号したチケットデータと前記暗号化チケットデータとその電子署名情報と前記受取者の公開鍵とを前記コンテンツ提供者装置に送付する手段と、前記コンテンツ提供者装置から送られてくる暗号化コンテンツ情報を受取者の秘密鍵で復号する手段とを備え、前記資格授与者装置は、前記コンテンツに関する要求情報に関連したチケットデータを受取者の公開鍵を用いて暗号化する手段と、その暗号化チケットデータに対し資格授与者の秘密鍵を用いて生成した電子署名情報を付す手段と、前記暗号化チケットデータとその電子署名情報を前記受取者装置に送付する手段とを備え、前記コンテンツ提供者装置は、資格授与者の公開鍵を用いて前記電子署名情報を検証する手段と、前記チケットデータを受取者の公開鍵で暗号化し、前記暗号化チ

ケットデータとの整合性を確認する手段と、受取者装置へ送るべきコンテンツ情報を受取者の公開鍵で暗号化し、その暗号化コンテンツ情報を前記受取者装置へ送付する手段とを備えたことを特徴とする。

【００１５】

さらに本発明は、上述のコンテンツ提供システムにおいて、前記コンテンツ提供者装置による前記暗号化チケットデータの整合性の確認後、受取者に関する情報取得の為の入力フォームを前記コンテンツ提供者装置から前記受取者装置に送る手段と、前記受取者装置において、前記入力フォームに対応する情報を受取者が入力することにより入力済みフォームを生成し、受取者の秘密鍵を用いて電子署名を施して前記コンテンツ提供者装置に送る手段と、前記コンテンツ提供者装置において、前記電子署名を受取者装置の公開鍵を用いて検証した後、前記コンテンツ情報を受取者の公開鍵で暗号化した暗号化コンテンツ情報を前記受取者装置へ送付する手段とをさらに備えたことを特徴とする。

【００１６】

さらに本発明は、上述のコンテンツ提供システムにおいて、前記資格授与者装置における前記受取者装置に前記暗号化チケットデータを送付する手段は、送付するデータに、資格授与者の公開鍵を含み資格授与者を客観的に証明する証明書を含め、前記受取者装置における前記コンテンツ提供者装置に前記チケットデータを送付する手段は、送付するデータに、前記資格授与者の証明書を含め、前記コンテンツ提供者装置における前記電子署名情報を検証する手段は、前記資格授与者の証明書を検証するとともに、前記資格授与者の電子署名情報を検証する際、前記資格授与者の証明書から取得した資格授与者の公開鍵を用いるものであることを特徴とする。

【００１７】

本発明によれば、正当な受取者のみが受取者装置で受取者の秘密鍵で復号することができないため、正当な受取者のみがコンテンツを受け取ることができる。

【００１８】

また、上記において、暗号化チケットデータの突き合わせチェックを行なった後に、コンテンツ提供者装置が受取者装置に記入フォームを送り、受取者がフォ

ームに記入した後に受取者の秘密鍵を用いて電子署名処理を施すことにより、コンテンツ提供者装置は正当な受取者から改ざんなしに記入済フォームを受け取ることが出来る。

【００１９】

【発明の実施の形態】

以下、図面を用いて、本発明の実施の形態を詳細に説明する。

【００２０】

図１は、本発明に係わるコンテンツ受取方法を適用したコンテンツ受取装置の一実施形態におけるシステム構成を示すブロック図である。本実施の形態では、インターネットビジネスとして電子懸賞を行う場合において、景品をデジタルコンテンツとした場合の受取を電子的に行うときのコンテンツ受取システムを一例として説明を行う。

【００２１】

図１に示すように、本システムは、受取者装置１００、資格授与者装置１１０、及びコンテンツ提供者装置１２０がネットワーク１３０を介して接続されて構成されている。受取者装置１００は、懸賞申込を行い、当選した場合には当該コンテンツを受け取ることになる受取者の計算機システムである。資格授与者装置１１０は、懸賞の募集を行い、懸賞受付や、抽選、当選発表を行い、当選者たる受取者にデジタルコンテンツを受け取ることを許可する許可証に相当するチケットデータを発行する資格授与者の計算機システムである。コンテンツ提供者装置１２０は、実際にデジタルコンテンツを管理し、正当な受取者に当該デジタルコンテンツを送るコンテンツ提供者により運用される計算機システムである。これらの装置１００～１２０の間で懸賞システムにおけるさまざまな情報がネットワーク１３０を介してやりとりされる。

【００２２】

各計算機システム１００～１２０としては、パーソナルコンピュータ、ワークステーションなどの現在一般に広く使われている計算機を用いることができる。また、これらの計算機は、より大型の、いわゆる汎用計算機で構成されてもよく、あるいは、その計算機が設けられる各機関におけるＬＡＮ等で接続された複数

の計算機からなる計算機システムとして構成されるものであっても、後述する計算機システムとしての機能を実現し得るものであればかまわない。なお、ネットワーク１３０に接続される計算機システムは図のように３つに制限されるわけではなく、任意の数の計算機システムが接続されていてよい。

【００２３】

図２は、受取者が使用する計算機システムである受取者装置１００の構成を示すブロック図である。なお、図においては、本実施の形態において、懸賞システムを実現する為に必要な機能構成を示している。受取者装置１００はその他の機能を備えていても良い。ここでは、本発明に直接的に関係していない機能については、特に図示せず、また、説明も省略する。

【００２４】

図２に示すように、受取者装置１００は、権利取得依頼入力部２０５、権利取得依頼メッセージ生成部２１０、鍵管理部２１５、チケットデータ受取確認部２２０、コンテンツ受取依頼メッセージ生成部２２５、暗号化コンテンツ復号部２３５、メッセージ送信部２４０、メッセージ受信部２４５、コンテンツ利用部２５０、画面出力部２５５、入力済みフォーム生成部２６０、及び電子署名付き入力済みフォーム生成部２６５を備えている。

【００２５】

権利取得依頼入力部２０５は、懸賞の応募者である受取者が取得したいコンテンツを特定する情報を入力する。本情報は事前に資格授与者から与えられていて、それを流用しても良い。

【００２６】

鍵管理部２１５は、受取者が所有する、誰にも開示してはならない鍵である受取者秘密鍵と、受取者秘密鍵と対になる第三者に開示しても良い鍵である受取者公開鍵を管理する。

【００２７】

権利取得依頼メッセージ生成部２１０は、権利取得依頼入力部２０５から取得した権利取得依頼データと、鍵管理部２１５から取得した受取者公開鍵とを連結し、資格授与者装置１１０へ送る為の権利取得依頼メッセージを生成して、メッ

セージ送信部２４０へ渡す。

【００２８】

チケットデータ受取確認部２２０は、メッセージ受信部２４５から暗号化されたチケットデータを受取り、鍵管理部２１５から受取者秘密鍵を取り出して暗号化されたチケットデータの復号を行う。受取者秘密鍵により復号が出来ることを確認することにより、チケットデータがそれを受け取った受取者にたいして与えられたものであることを確認できる。

【００２９】

コンテンツ受取依頼メッセージ生成部２２５は、チケットデータ受取確認部２２０により復号したチケットデータを受取るとともに、メッセージ受信部２４５より電子署名付き暗号化チケットデータを受取り、コンテンツ受取者装置１１０へ送る為のコンテンツ受取依頼メッセージを生成してメッセージ送信部２４０へ渡す。

【００３０】

暗号化コンテンツ復号部２３５は、メッセージ受信部２４５から暗号化コンテンツを受け取り、鍵管理部２１５から受取者公開鍵を取得し、復号を行う。また復号を行ったコンテンツをコンテンツ利用部２５０へ渡す。

【００３１】

入力済みフォーム生成部２６０は、メッセージ受信部２４５から受け取った入力フォームを用いてデータを入力し、入力済みフォームを生成する。電子署名付き入力済みフォーム生成部２６５は、入力済みフォーム生成部２６０から受け取った入力済みフォームに鍵管理部２１５から取得した受取者秘密鍵を用いて電子署名を施し、電子署名付き入力済みフォームを生成し、メッセージ送信部２４０へ送る。

【００３２】

図３は、資格授与者の計算機システムである資格授与者装置１１０の構成を示すブロック図である。なお、図においては、本実施の形態において、懸賞システムを実現する為に必要な機能構成を示している。資格授与者装置１１０はその他の機能を備えていても良い。ここでは、本発明に直接的に関係していない機能に

ついては、特に図示せず、また、説明も省略する。

【００３３】

図３に示すように、資格授与者装置１１０は、メッセージ受信部３０５と、抽選部３１０と、チケットデータ管理部３１５と、チケットデータ暗号部３２０と、暗号化チケットデータ署名部３２５と、メッセージ送信部３３０と、鍵・証明書管理部３３５とを備えている。

【００３４】

抽選部３１０は、メッセージ受信部３０５から受け取った権利取得依頼に関して、前記依頼を当選させコンテンツ受け取り資格を与えるかどうかを判断する。

【００３５】

チケットデータ暗号部３２０は、抽選部３１０が資格を与えると判断した場合に、権利取得依頼メッセージを元に、チケットデータ管理部３１５からチケットデータを取り出し、前記チケットデータを権利取得依頼メッセージ付属の受取者公開鍵を用いて暗号化し、前記チケットデータを、権利を与えた受取者のみが権利行使出来るようにする。チケットデータ管理部３１５は、正当な資格を与えるためのチケットデータを管理している。

【００３６】

暗号化チケットデータ署名部３２５は、チケットデータ暗号部３２０で生成した暗号化チケットデータに対し、その暗号化チケットデータを資格授与者が生成したことを証明する電子署名データを鍵・証明書管理部３３５から取得した資格授与者秘密鍵を用いて生成し、付与する。また、資格授与者秘密鍵に対応した資格授与者公開鍵が、確かに資格授与者のものであることを、コンテンツ提供者承認の機関が承認していることを示す、資格授与者証明書を付与する。本資格授与者証明書には、資格授与者公開鍵が含まれている。生成した電子署名つき暗号化チケットデータは、メッセージ送信部３３０に渡される。

【００３７】

図４は、コンテンツ提供者の計算機システムであるコンテンツ提供者装置１２０の構成を示すブロック図である。なお、図においては、本実施の形態において、懸賞システムを実現する為に必要な機能構成を示している。コンテンツ取扱者

装置１２０はその他の機能を備えていても良い。ここでは、本発明に直接的に関係していない機能については、特に図示せず、また、説明も省略する。

【００３８】

図４に示すように、コンテンツ提供者装置１２０は、メッセージ受信部４０５と、暗号化チケットデータ電子署名検証部４１０と、チケットデータ暗号部４１５と、突合わせチェック部４２０と、受取者データ保管部４２５と、入力フォーム生成部４３０と、入力済みフォーム電子署名検証部４３５と、コンテンツ管理部４４０と、コンテンツ暗号部４４５と、メッセージ送信部４５０とを備えている。

【００３９】

暗号化チケットデータ電子署名検証部４１０は、メッセージ受信部４０５から受け取ったコンテンツ受取依頼メッセージに含まれている暗号化チケットデータに関する電子署名情報を検証し、暗号化チケットデータが正当であること、つまり資格を与えても良い資格授与者から発行されていることをチェックする。

【００４０】

チケットデータ暗号部４１５は、メッセージ受信部４０５からチケットデータと受取者公開鍵を受け取り、チケットデータを前記受取者公開鍵を用いて暗号化する。チケットデータ暗号部４１５で生成された暗号化チケットデータは、公開鍵が抽選申込時に使用されたものであるかどうかを検証するために、メッセージ受信部４０５から渡された暗号化チケットデータと突き合わせ検証部４２０にて突き合わせ検証される。

【００４１】

入力済みフォーム電子署名検証部４３５は、メッセージ受信部４０５から受け取った入力済みフォームに関する電子署名を、データ保管部４２５から受取者公開鍵を取得して検証を行なった後に、当該入力済みフォームをデータ保管部４２５へ格納する。

【００４２】

コンテンツ暗号部４４５は、データ保管部４２５に保管していたチケットデータからコンテンツ管理部４４０にて管理している関連コンテンツを取り出し、デ

ータ保管部４２５に保管していた受取者公開鍵で暗号化してメッセージ送信部４５０へ渡す。本暗号化コンテンツは暗号化した受取者公開鍵と対になる受取者秘密鍵の所有者のみしか復号できない為、コンテンツを資格授与者装置１１０が授与した正当な受取者装置１００のみへ安全に渡すことが出来る。

【００４３】

図５は、本実施の形態のコンテンツ受取システムにおけるメッセージのやりとりを示した全体フロー図である。

【００４４】

受取者装置１００は、懸賞に応募する為の情報をあらかじめ資格授与者装置１１０から取得しているものとする。また、公開鍵と、それに対応する秘密鍵も、事前に鍵管理部２１５に保持しているものとする。

【００４５】

ステップ５１０にて、受取者装置１００は、権利取得要求メッセージを資格授与者装置１１０へ送るために、権利取得依頼入力部２０５にて抽選に参加したい対象のコンテンツ情報を設定し、権利取得要求情報を生成する。その後、鍵管理部２１５から受取者公開鍵を取り出し、受取者公開鍵と権利取得要求情報から権利取得要求メッセージを生成し、ステップ５１０にて資格授与者装置１１０へ送る。

【００４６】

図６は、資格授与者装置１００へ送る権利取得要求メッセージのデータ構成図である。権利取得要求メッセージ７００は、権利取得要求情報７１０と受取者公開鍵７２０から構成される。

【００４７】

資格授与者装置１１０は、権利取得要求メッセージ７００を受信後、抽選部３１０にて当該要求を当選と扱うか落選と扱うかを決定する(ステップ５１２)。落選の場合は、落選したことを示す情報を受取者装置１００へ送付し、終了する。当選の場合は、権利取得要求情報７１０と関連したチケットデータをチケットデータ管理部３１５から取得する。

【００４８】

図７は、チケットデータのデータ構成図である。チケットデータ９００は、コンテンツ提供者装置１２０の所在を示すコンテンツ提供者アドレス９１０とコンテンツ提供者装置１２０が提供すべきコンテンツを識別する為に使用するコンテンツ識別情報９２０から構成される。

【００４９】

次に、チケットデータ９００を受取者公開鍵７２０を用いて暗号化する(ステップ５１４)。これにより、暗号化チケットデータ１０１０の復号が、受取者公開鍵７２０と対になる受取者秘密鍵を保持する受取者、つまり当選した受取者装置１００のみにしかできないようにする。その後、資格授与者が当該データを生成したことを保証する為に、鍵・証明書管理部３３５から資格授与者秘密鍵を取り出し、生成した暗号化チケットデータへ電子署名を施し、前記資格授与者秘密鍵と対になる資格授与者公開鍵を含む証明書を付与する(ステップ５１６)。このようにして生成した署名付き暗号化チケットデータ１０００を受取者装置１００へ送る(ステップ５２０)。

【００５０】

ここで、電子署名は、所定のハッシュ関数を用いて受渡データ、ここでは暗号化チケットデータのハッシュ値を取得し、自己の秘密鍵で暗号化して得られた情報である。ハッシュ関数とは、元のデータと一意に結びつけることができ、かつデータ量を削減したデータを作成することができる一方向性関数である。また、証明書は、第三者により発行され、その所持者を客観的に証明するための情報である。ここでは、認証される機関が使用する自己秘密鍵情報に対応した公開鍵情報に対し、第三者の秘密鍵情報で電子署名を施したデータであり、電子署名時には電子署名を行なった機関を特定することが出来る。

【００５１】

図８は、署名付き暗号化チケットデータのデータ構成図である。署名付き暗号化チケットデータ１０００は、チケットデータ９００を受取者の公開鍵７２０で暗号化した暗号化チケットデータ１０１０と、暗号化チケットデータ１０１０に対して電子署名を施した資格授与者電子署名１０２０と、資格授与者の証明書が設定される資格授与者証明書１０３０とから構成される。

【００５２】

なお本実施の形態では、資格授与者装置１１０は、権利取得要求情報７１０を受け取った後、直ちに抽選を行ない、署名付き暗号化チケットデータ１０００を返しているが、資格授与者装置１１０は、例えば一旦複数の受取者装置から権利取得要求メッセージを受理し、一定の期間後にまとめて抽選を行ない、当選者に対して署名付き暗号化チケットデータ１０００を送付することとしてもよい。この場合、署名付き暗号化チケットデータ１０００は、電子メールにて受取者装置１００に送ってもよいし、WWW上に公開して、受取者装置１００がWWWサーバにアクセスして取得しても良い。この場合、当選者以外の受取者が署名付き暗号化チケットデータ１０００を取得したとしても、当該当選者の秘密鍵を持っていなければ復号できない。

【００５３】

図５に戻って、受取者装置１００は、署名付き暗号化チケットデータ１０００を受け取った後、鍵管理部２１５から受取者秘密鍵を取り出し、チケットデータ受取確認部２２０により暗号化チケットデータ１０１０に対する復号処理を行なう(ステップ５２５)。受取者装置１００は、その際にチケットデータ９００の内容を画面出力により確認してもよい。その後、コンテンツ受取依頼メッセージ生成部２２５にて、復号に用いた受取者公開鍵と復号したチケットデータとを、署名付き暗号化チケットデータ１０００に付与し、コンテンツ提供者１２０へ送る(ステップ５３０)。その際、コンテンツ提供者装置１２０へは、チケットデータ９００内のコンテンツ提供者アドレス９１０を用いてメッセージを送る。

【００５４】

図９は、コンテンツ受取依頼メッセージのデータ構成図である。コンテンツ受取依頼メッセージ１２００は、電子署名つき暗号化チケットデータ１０００にチケットデータ１２１０と受取者公開鍵１２２０(実際には受取者公開鍵７２０と同様の鍵)が付加されて構成される。

【００５５】

コンテンツ提供者装置１２０は、コンテンツ受取依頼メッセージ１２００を受け取った後、暗号化チケットデータ１０１０が、コンテンツ提供者装置１２０か

らみて正当な資格授与者が発行しているものかどうかを確認する為に、ステップ５３３において、資格授与者証明書１０３０を用いて資格授与者電子署名１０２０に関して電子署名検証部４１０により電子署名検証を行ない、その結果を判定する。この確認は、証明書がコンテンツ提供者と契約関係のある資格授与者のものかどうかの確認と、証明書から得られた資格授与者の公開鍵情報を使って電子署名を復号して得られるハッシュ値と暗号化チケットデータ１０１０から得られるハッシュ値とを比較することにより行われる。この判別の結果、暗号化チケットデータまたは資格授与者電子電子署名のいずれかが不当である場合は、エラー処理を実施し処理を終了する。

【００５６】

ステップ５３３において電子署名の妥当性が検証された後、チケットデータ暗号部４１５にてチケットデータ１２１０を受取者公開鍵１２２０で暗号化し、暗号化チケットデータ１０１０と突き合わせ検証を行ない、その結果を判定し、受取者公開鍵１２２０が、抽選申込時に使用され、資格授与者装置１１０が暗号化チケットデータの生成に用いた公開鍵７２０と同一かどうかを確認する(ステップ５３６)。この判別の結果、一致しなかった場合は、エラー処理を実施して処理を終了する。

【００５７】

ステップ５３６において、受取者公開鍵１２２０が、抽選申込時に使用され、資格授与者装置１１０が暗号化チケットデータ１０１０の生成に用いた受取者公開鍵７２０と同一であった場合、データ保管部４２５内のチケットデータ９００のコンテンツ識別情報９２０を用いてコンテンツ管理部４４０から該当コンテンツを取り出し、コンテンツ暗号部４４５で受取者公開鍵７２０(または１２２０)を用いて当該コンテンツを暗号化し(ステップ５５５)、暗号化コンテンツを受取者装置１００へ返す(ステップ５６０)。

【００５８】

受取者装置１００は、コンテンツ提供者装置１２０から暗号化コンテンツを受け取り、鍵管理部２１５から受取者秘密鍵を取得し、暗号化コンテンツ復号部２３５にて暗号化コンテンツを復号し、コンテンツをコンテンツ利用部２５０に渡

してコンテンツを利用する。

【００５９】

上述の実施の形態において、ステップ５３６の結果、暗号化チケットデータの突き合わせが一致した場合、必要ならばコンテンツ提供者が受取者からアンケート等の受取者情報を受け取る為の受取者情報取得フェーズ(５７０)を行なうようにしてもよい。この場合、コンテンツ提供者装置１２０は、受け取りたい情報に関する入力フォームを生成し、受取者装置１００へ送る(ステップ５４０)。受取者装置１００は入力フォームを画面出力部２５５にて表示し、受取者は表示内容にしたがって、入力装置から必要な情報を入力し、入力済みフォームを生成し、受取者秘密鍵を用いて入力済みフォームに対して電子署名を生成して付加し、ステップ５５０にてコンテンツ提供者装置へ送る。コンテンツ提供者装置１２０は、データ保管部４２５から受取者公開鍵を取得し、電子署名検証を行ない、入力フォーム記入者が当選者であることを確かめ、記入データをデータ保管部４２５へ保管する。なお受取者情報取得フェーズ(５７０)は、必要ならば繰り返すことが出来る。

【００６０】

上述の実施の形態では懸賞商品としてデジタルコンテンツを用いたが、商品としては物品でもよい。この場合、配送先情報のなりすましを避ける為に配送先情報等は受取者情報取得フェーズ(５７０)を用いて行う。

【００６１】

上述の実施の形態においては、電子懸賞における、景品をデジタルコンテンツとした場合の受取を電子的に行う場合のコンテンツ受取システムに関して述べたが、クレジットカードのポイントを用いてのデジタルコンテンツの配送システムとしても本発明を適用することができる。

【００６２】

【発明の効果】

以上述べたように、本発明によれば、受取資格授与者たる第三者機関が授与対象コンテンツデータを管理することを避け、当該受取者のみが安全に受け取ることができる。また、資格授与者側とコンテンツ提供者間は事前に受取者情報を直

接やりとりする必要はなく、コンテンツ提供者は事前に受取者に関するアクセスの為のパスワード管理などのデーターベースを構築する必要はない。また、コンテンツ提供者装置は正当な受取者から改ざんなしに記入済フォームを受け取ることが出来る。これは特にコンテンツ提供者が物品を受取者へ郵送する場合に、住所などの情報を正当な受取者から取得することに対して有効である。

【図面の簡単な説明】

【図１】

本発明に係わるコンテンツ受取方法を適用したコンテンツ受取装置の一実施形態におけるシステム構成を示すブロック図である。

【図２】

受取者の計算機システムである受取者装置の構成を示すブロック図である。

【図３】

資格授与者の計算機システムである資格授与者装置の構成を示すブロック図である。

【図４】

コンテンツ取扱者の計算機システムであるコンテンツ取扱者装置の構成を示すブロック図である。

【図５】

インターネットビジネスにおいて、電子懸賞における景品をデジタルコンテンツとし受取を電子的に行う場合のコンテンツ受取システムを実現する場合のメッセージのやりとりを示した全体フロー図である。

【図６】

資格授与者装置へ送る権利取得要求メッセージのデータ構成図である。

【図７】

チケットデータのデータ構成図である。

【図８】

電子署名つき暗号化チケットデータのデータ構成図である。

【図９】

コンテンツ受取依頼メッセージのデータ構成図である。

【符号の説明】

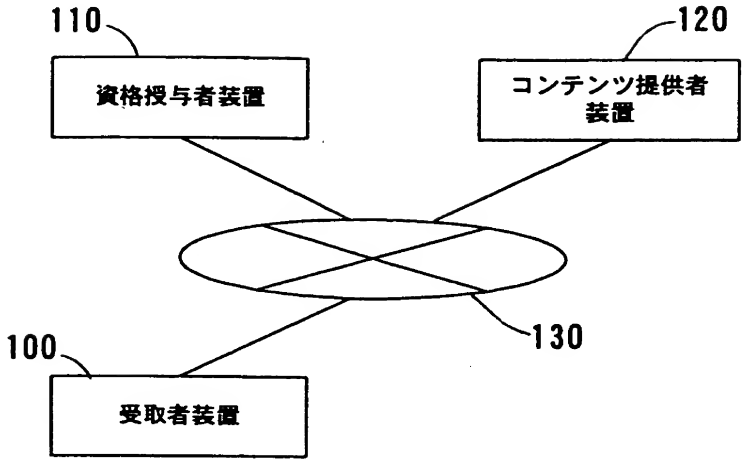
１００…受取者装置

１１０…資格授与者装置

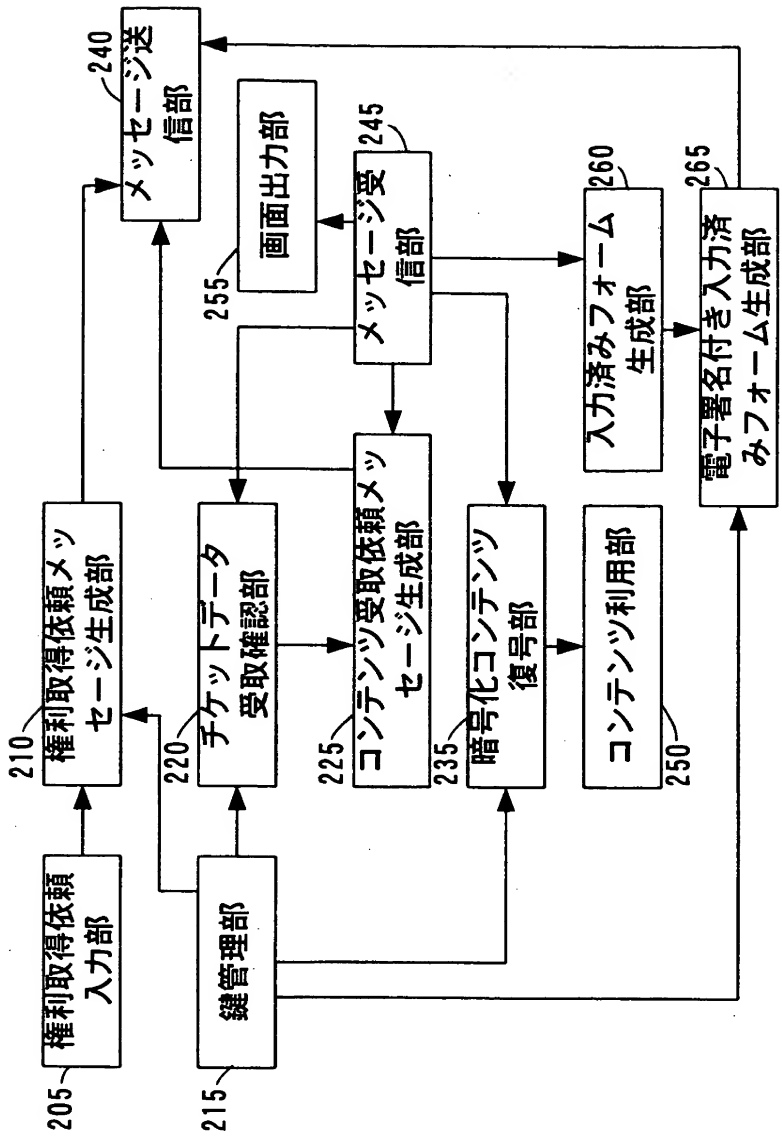
１２０…コンテンツ提供者装置

【書類名】　図面

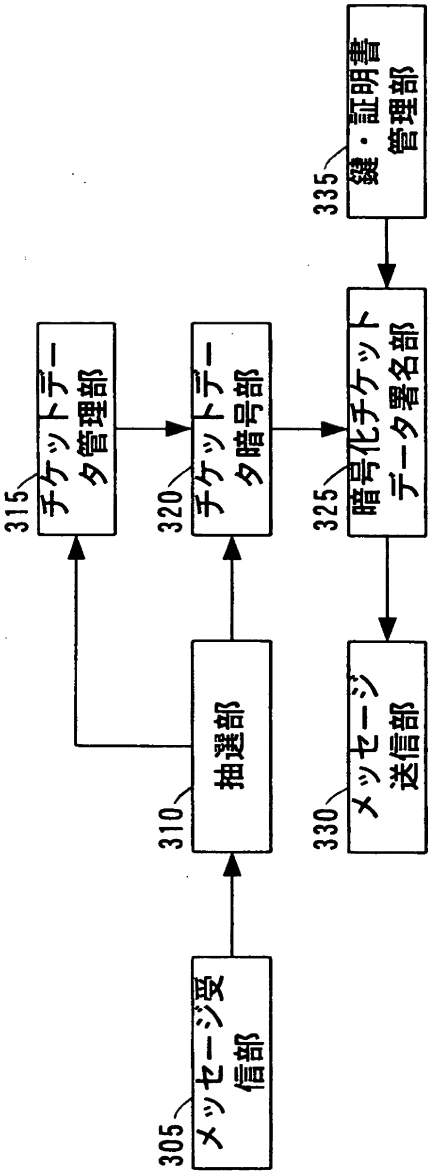
【図１】



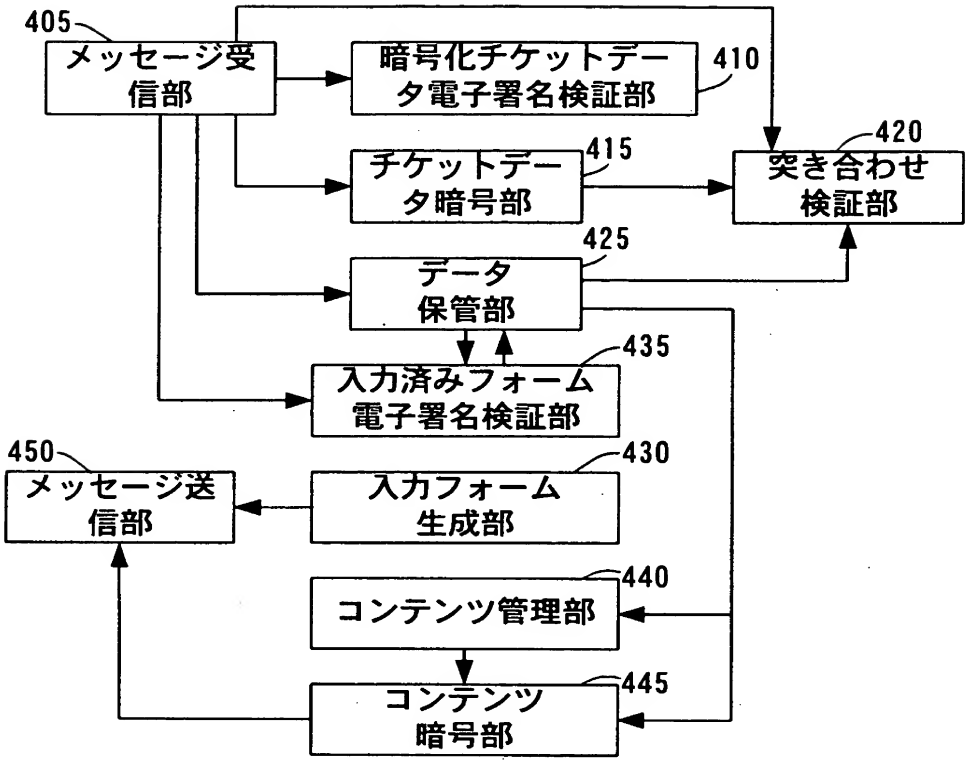
【図２】


権利取得依頼入力部
205
権利取得依頼メッセージ生成部
210
鍵管理部
215
チケットデータ受取確認部
220
コンテンツ受取依頼メッセージ生成部
225
暗号化コンテンツ復号部
235
コンテンツ利用部
250
画面出力部
255
メッセージ送信部
240
メッセージ受信部
245
入力済みフォーム生成部
260
電子署名付き入力済みフォーム生成部
265

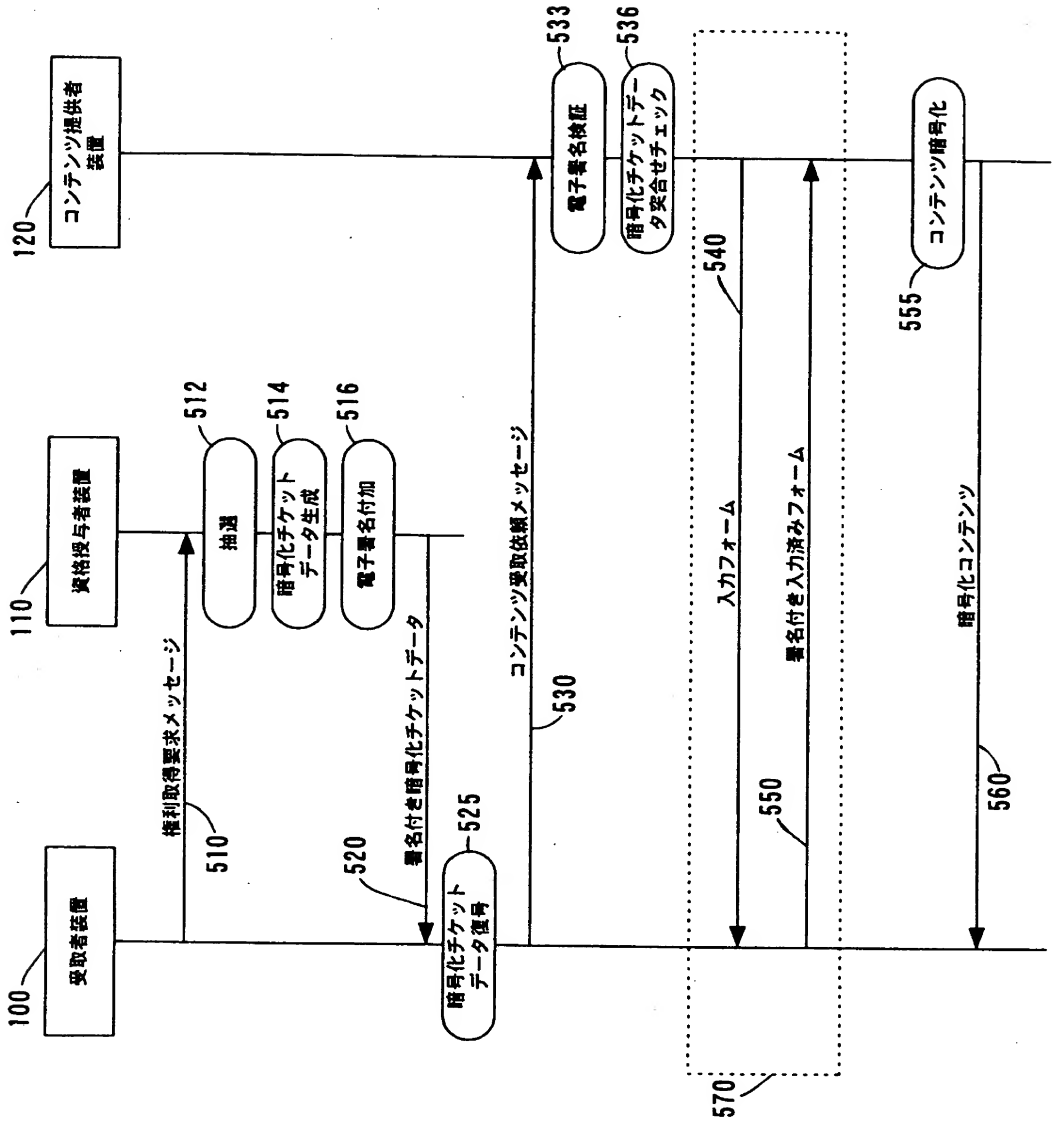
【図３】


鍵・証明書管理部
335
チケットデータ管理部
315
チケットデータ暗号部
320
暗号化チケットデータ署名部
325
抽選部
310
メッセージ送信部
330
メッセージ受信部
305

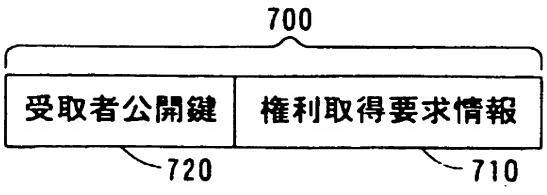
【図４】


405
メッセージ受信部
暗号化チケットデータ電子署名検証部
410
420
突き合わせ検証部
チケットデータ暗号部
415
425
データ保管部
435
入力済みフォーム電子署名検証部
450
メッセージ送信部
430
入力フォーム生成部
440
コンテンツ管理部
445
コンテンツ暗号部

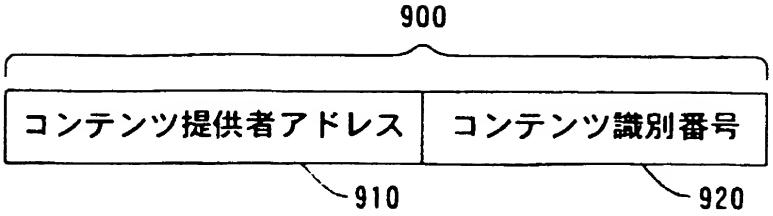
【図５】


コンテンツ提供者装置
120
533
電子署名検証
536
暗号化チケットデータ突合せチェック
555
コンテンツ暗号化
540
入力フォーム
署名付き入力済みフォーム
550
暗号化コンテンツ
560
570
資格授与者装置
110
512
抽選
514
暗号化チケットデータ生成
516
電子署名付加
コンテンツ受取依頼メッセージ
530
権利取得要求メッセージ
510
署名付き暗号化チケットデータ
520
525
暗号化チケットデータ復号
受取者装置
100

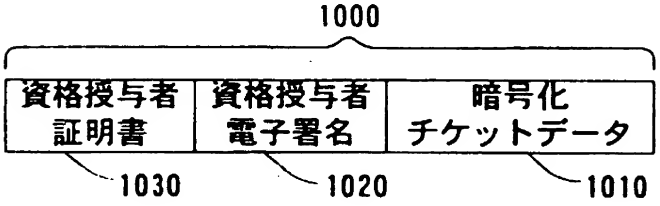
【図６】


700
受取者公開鍵
権利取得要求情報
720
710

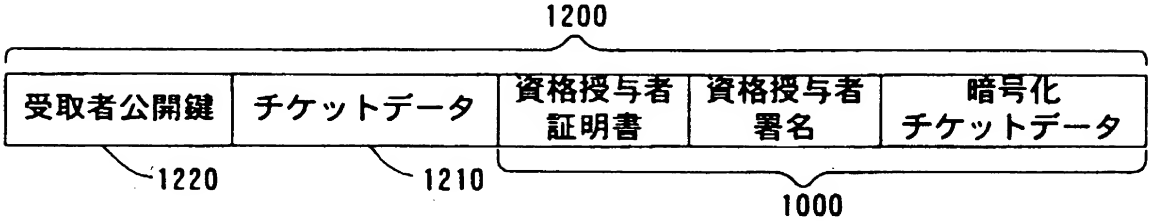
【図７】


900
コンテンツ提供者アドレス
コンテンツ識別番号
910
920

【図８】


1000
資格授与者証明書
資格授与者電子署名
暗号化チケットデータ
1030
1020
1010

【図９】


1200
受取者公開鍵
チケットデータ
資格授与者証明書
資格授与者署名
暗号化チケットデータ
1220
1210
1000

【書類名】　要約書

【要約】

【課題】

コンテンツ受取者と提供者の二者間において、通信ネットワークを用いて各種のコンテンツを授受する際に、コンテンツの受取資格授与者と提供者を明確に分離することにより受取資格授与者が授与対象コンテンツデータを管理することを避け、その上で受取資格授与者が権利を与えた当該受取者のみが安全に受け取ることができるようにすること、および正当なコンテンツ受取者からの情報を当該コンテンツ受取者からの情報だと認識しつつ、コンテンツ提供者が受け取ることができるようにすることを目的とする。

【解決手段】

受取者装置において、受取者の公開鍵と、受取依頼要求情報を、権利取得要求メッセージとして資格授与者装置に送る。資格授与者装置では、受け取った受取依頼要求情報から該当するチケットデータを受取者の公開鍵で暗号化し、その暗号化チケットデータに電子署名を付与した電子署名つき暗号化チケットデータを受取者装置へ返す。受取者装置では受け取ったデータの暗号化チケットデータ部分を受取者の秘密鍵を用いて復号し、前記チケットデータと受取者の公開鍵を電子署名つき暗号化チケットデータに付与してコンテンツ受取依頼メッセージとしてコンテンツ提供者装置へ送る。コンテンツ提供者装置は暗号化チケットデータの電子署名を検証した後、受取者装置から受け取ったチケットデータを受取者の公開鍵で暗号化し、受取者装置から受け取った暗号化チケットデータと突き合わせ検証を行なうことにより、正当な受取者であることを確認し、コンテンツデータを受取者の公開鍵で暗号化して送る。

【選択図】　図５

認定・付加情報

特許出願の番号	特願２０００－２１８４０８
受付番号	５００００９１２１８７
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１２年　７月２１日

＜認定情報・付加情報＞

【提出日】　平成12年 7月19日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所